**Amendments to the Specification:**

Page 2, line 3

~~**COULD YOU TELL ME WHAT THE ACRONYM PARTIES STANDS FOR?**~~

Page 2, line 5

Figure 2 depicts a conventional method 50 for using a sub-partition of a lockable, nonviewable partition as a boot source. The method 50 is described in conjunction with the computer system 10. Referring to Figures 1 and 2, the method 50 may be carried out upon start-up of the computer system 10, using the basic input output system (BIOS) of the computer system 10 (not shown in Figure 1). The hardfile 30 is accessed, via step 52. Step 52 could include using the BIOS to read the boot record 32 and determine the identity of the partition 20 and the sub-partitions 22, 24, 26 and 28. The user is queried as to which sub-partitions 22, 24, 26 and 28 to use in booting the computer system 10, via step 54. The user then selects one of the sub-partitions 22, 24, 26 and 28 to be the boot source for the computer system 10, via step 56. The user can select any one of the sub-partitions 22, 24, 26 and 28 as the boot source in step 56. The computer system 10 then boots from the selected sub-partition 22, 24, 26 or 28, via step 58. Thus, the computer system 10 can boot from a particular sub-partition 22, 24, 26 or 28.

Page 6, line 23

Because the sub-partitions 112, 114, 116 and 118 are each protected by a password, access can be restricted to users having the corresponding password. As a result, the sub-partitions 112, 114, 116 and 118 can be trusted boot sources for the computer system. Not every user having access to the partition 110 can boot using all sub-partition 112, 114, 116 and 118. Instead, a user can be given a password for sub-partitions 112, 114, 116 or 118 that correspond to the user's level of security. For example, a system administrator may have the password for all sub-partitions 112, 114, 116 and 118, including those that allow the computer system 100 to be reconfigured. A user of the computer system 100 may, however, be provided with a password to one or two of the sub-partitions 112, 114, 116 and 118. Thus, the user can still boot the computer system 100 using the partition 110, but may not be able to reconfigure the computer system 100. Thus, secure boot sources can be provided for the computer system 100 in the partition ~~100~~110, while allowing users having lower level security clearance access to one or more of the sub-partitions 112, 114, 116 and 118.

Page 7, line 13

Figure 5 depicts a more detailed flow chart of a method 210 for providing a trusted boot source. The method 210 is preferably used in conjunction with the computer system 100. Consequently, the method 210 will be described in the context of the computer system 100. Referring to Figures 3 and 5, the plurality of sub-partitions 112, 114, 116 and 118 in the partition 110 are identified, via step 212. Step 212 is analogous to the step 202 of the method 200 depicted in Figure 4. Referring back to Figures 3 and 5, step 212~~02~~ preferably provides the definitions 124 of the sub-partitions 112 114, 116 and 118. A password for each of the sub-partitions 112, 114, 116 and 118 is provided, via step 214. The password for a sub-partition 112, 114, 116 or 118 is required for a user to boot the computer system 100 using the sub-partition 112, 114, 116 or 118. In one embodiment, the passwords provided in step 214 could include an additional password for the partition 110. Thus, in one embodiment, a user will need two passwords, one for the partition 110 and one for the sub-partition 112, 114, 116 or 118 that the user will utilize in booting the computer system 100. The passwords provided in step 214 are preferably stored in the list 122 of the boot record 122.

Page 8, line 19

Thus, the method 210 allows a user to boot from one of the sub-partitions 112, 114, 116 or 118 if the user provides the corresponding password. Because each of the sub-partitions 112, 114, 116 and 118 can be protected by a password, the sub-partitions 112, 114, 116 and 118 can be trusted boot sources for the computer system. Not every user having access to the partition 110 can boot using all sub-partition 112, 114, 116 and 118. Instead, a user can boot using the sub-partitions 112, 114, 116 or 118 and have access to the utilities provided through the sub-partitions 112, 114, 116 and 118 only if the user has the corresponding password. Thus, certain utilities can be restricted for use by some users. For example, a system administrator may have the password for all sub-partitions 112, 114, 116 and 118, including those that allow the computer system 100 to be reconfigured. Other users of the computer system 100 may, however, be provided with a password to one of the sub-partitions 112, 114, 116 and 118 that does not provide the utilities for reconfiguring the computer system 100. The user can still boot the computer system 100, but may not be able to reconfigure the computer system 100. Thus, secure boot sources can be provided for the computer system 100 in the partition ~~100~~100, while allowing users having lower level security clearance access to one or more of the sub-partitions 112, 114, 116 and 118.